Public key certificate

From Wikipedia, the free encyclopedia.
(Redirected from Digital identity certificate)

In cryptography, a **public key certificate** (or **identity certificate**) is a certificate which uses a digital signature to bind together a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). In a web of trust scheme, the signature is of either the user (a self-signed certificate) or other users ("endorsements"). In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together.

Use

Certificates can be used for the large-scale use of public-key cryptography. Securely exchanging secret keys amongst users becomes impractical to the point of effective impossibility for anything other than quite small networks. Public key cryptography provides a way to evade this problem. In principle, if Alice wants others to be able to send her secret messages, she need only publish her public key. Anyone possessing it can then send her secure information. Unfortunately, Mallory can also publish a public key (for which he knows the related private key) claiming it is Alice's and so receive at least some of the secret messages meant for her. But if Alice builds her public key into a certificate and has it digitally signed by a trusted third party (Trent), anyone who trusts Trent can merely check the certificate to see whether Trent thinks the embedded public key is Alice's. In typical PKIs, Trent will be a CA, who is trusted by all participants. In a web of trust, Trent can be any user, and whether to trust that user's attestation that a particular public key belongs to Alice will be up to the person wishing to send a message to Alice.

In large-scale deployments, Alice may not be familiar with Bob's certificate authority (perhaps they each have a different CA — if both use employer CAs, different employers would produce this result), so Bob's certificate may also include his CA's public key signed by a "higher level" CA_2, which might be recognized by Alice. This process leads in general to a hierarchy of certificates, and to even more complex trust relationships. Public key infrastructure refers, mostly, to the software that manages certificates in a large-scale setting. In X.509 PKI systems, the hierarchy of certificates is always a top-down tree, with a root certificate at the top, representing a CA that is 'so central' to the scheme that it does not need to be authenticated by some trusted third party.

A certificate may be revoked if it is discovered that its related private key has been compromised, or if the relationship (between an entity and a public key) embedded in the certificate is discovered to be incorrect or has changed; this might occur, for example, if a person changes jobs or names. A revocation will likely be a rare occurrence, but the possibility means that when a certificate is trusted, the user should always check its validity. This can be done by comparing it against a certificate revocation list (CRL) — a list of revoked or cancelled certificates. Ensuring that such a list is up-to-date and accurate is a core function in a centralized PKI, one which requires both staff and budget and one which is therefore sometimes not properly done. To be effective, it must be readily available to any who need it whenever it is needed and must be updated frequently. The other way to check a certificate validity is to query the certificate authority using the Online Certificate Status Protocol (OCSP) to know the status of a specific certificate.

A certificate typically includes:

- The public key being signed.

- A name, which can refer to a person, a computer or an organization.
- A validity period.
- The location (URL) of a revocation center.

The most common certificate standard is the ITU-T X.509. X.509 is being adapted to the Internet by the IETF PKIX work-group.

See also

- OpenPGP
- Secure Sockets Layer, Transport Layer Security
- Authorization certificate

External links

- Netscape's Introduction to Public-Key Cryptography (http://developer.netscape.com/docs/manuals/security/pkin/contents.htm)

Retrieved from "http://en.wikipedia.org/wiki/Public_key_certificate"

Categories: Cryptography | Computer security | Electronic commerce

Root certificate

From Wikipedia, the free encyclopedia.

In cryptography and computer security, a **root certificate** is an unsigned public key certificate, or a self-signed certificate, and is part of a PKI scheme. The most common commercial variety is based on the ISO X.509 standard. Normally an X.509 certificate includes a digital signature from a certificate authority (CA) which vouches for correctness of the data contained in a certificate.

The authenticity of the CA's signature, and whether the CA can be trusted, can be determined by examining its certificate in turn. This chain must however end somewhere, and it does so at the *root certificate*, so called as it is at the root of a tree. (A CA can issue multiple certificates, which can be used to issue multiple certificates in turn, thus creating a tree).

Root certificates are implicitly trusted. They are included with many software applications. The best known is Web browsers; they are used for SSL / TLS secure connections. However this implies that you trust your browser's publisher to include correct root certificates, and in turn the certificate authorities it trusts, and any one the CA may have issued a certificate-issuing-certificate to, to faithfully authenticate the users of all their certificates. This (transitive) trust in a root certificate is merely assumed in the usual case, there being no way in practice to better ground it, but is integral to the X.509 certificate chain model.

Retrieved from "http://en.wikipedia.org/wiki/Root_certificate"

Categories: Cryptography

How to protect the company jewels

August 20, 1998
Web posted at: 2:20 PM EDT

by William Stallings

From... NetworkWorld Fusion ANSWERS IDG.net

(IDG) -- Some of the most versatile network security tools are public-key cryptography and the use of certificate authorities (CA) to ensure the secure transmission of data across an intranet or the Internet. One scheme has become universally accepted for formatting public-key certificates: the X.509 standard. X.509 certificates are used in most network security applications, including IP Security (IPSec), Secure Sockets Layer (SSL), Secure Electronic Transaction (SET) and Secure Multi-purpose Internet Mail Extensions (S/MIME).

In the X.509 scheme, a user has two keys: a private key known only to the user, and a public key, which is publicly available to other users. Public-key cryptography has two main uses: key distribution and authentication. A user can encrypt a message with a conventional key, such as a Data Encryption Standard key, and then encrypt the DES key with the public key of the recipient and attach that to the message. The recipient can use the matching private key to recover the DES key, and then decrypt the message.

For authentication, X.509 and public-key cryptography provide for a device called the digital signature. A user can create a message and generate a digest, or fingerprint, of the message. The user encrypts the digest with his private key to form the signature. The recipient can use the sender's public key to decrypt the signature and match it against the fingerprint of the incoming message to assure authenticity.

Although public-key cryptography is virtually unbreakable with the proper algorithm and sufficient key length, there is one vulnerability: How does a recipient know that someone else's public key is valid?

Solving the problem

The solution to this problem is X.509 and the public-key certificate. In essence, a certificate consists of a public key plus a user identification of the key owner, with the whole block signed by a dependable third party. Typically, the third party is a CA that is trusted by the user community, such as a government agency or financial institution.

A user can present his public key to the CAin a secure manner to obtain a certificate. The user can then publish the certificate, and anyone who needs this user's public key can obtain the certificate and verify the key is valid by way of the

CA.

The public-key certificate makes use of public-key encryption technology to protect and validate public keys. For this purpose, a user must apply to a CA to create the key. The user supplies his public key plus some sort of unique user identifier.

The public key and user ID, together with a CA identification, form the unsigned certificate. The CA then takes the hash code of this unsigned certificate. A hash code is a small block of data that serves as a sort of fingerprint. For all practical purposes, two different certificates will yield two different hash codes.

Next the CA encrypts the hash code with the CA's private key to produce the signature. A common public-key algorithm for this purpose comes from RSA Data Security. Because only the CA possesses its private key, only the CA could produce this signature. The CA attaches the signature to the certificate to form the signed certificate.

The user may supply this certificate to anyone who needs the user's public key. To verify that a public key is valid, the recipient recovers the hash code from the signature by decrypting the signature using the CA's public key.

Then, the recipient calculates the hash code of the unsigned certificate and compares this to the hash code recovered from the signature. If the two codes match, this is a valid certificate and the recipient may trust that the public key in that certificate belongs to the identified user.

Additional features

In addition to the user's identifier, the user's public key and the CA's identifier, an X.509 certificate includes several other elements. The certificate contains an identifier of the algorithm used to sign the certificate and the period of validity of the certificate. The latest version of the standard, X.509v3, also includes an extensions field to provide more flexibility and to convey information needed in special circumstances.

Finally, X.509 provides a format for use in revoking a key before it expires. This enables a user to cancel a key at any time.

Stallings is a consultant, lecturer and author on data communications and networking topics. This article is based on material in his most recent book, Cryptography and Network Security. He can be reached at ws@shore.net.

Related stories:

- The long, strong arm of the NSA - xxxxxxxx
- Hole in Internet security discovered - June 30, 1998
- Government restrictions on encryption pose obstacles for Internet security - May 18, 1998

Related IDG.net stories:

Note: Pages will open in a new browser window

- Gov't restrictions on encryption pose obstacles for Net security (*Network World Fusion*) *Free registration required to view this site.*
- Clinton's encryption policy (*InfoWorld*)
- 13 companies support encryption alternative (*Network World Fusion*) *Free registration required to view this site.*
- International experts see need for global encryption policy (*InfoWorld*)
- Crypto experts blast Clinton (*Network World Fusion*) *Free registration required to view this site.*
- The problem with certification *Free registration required to access this site.* (*Network World Fusion*)
- Certificates merit a look *Free registration required to access this site.* (*Network World Fusion*)
- SSL makes headway as an encryption standard (*Netscape Enterprise Developer*)

Related sites:

- National Security Agency

External sites are not endorsed by CNN Interactive.
